Outline for October 20, 2003

Reading: Chapters 9.3—9.4

Discussion Problem

> "To fight and conquer in all your battles is not supreme excellence; supreme excellence consists in breaking the enemy's resistance without fighting. In the practical art of war, the best thing of all is to take the enemy's country whole and intact; to shatter and destroy it is not so good. So, too, it is better to capture an army entire than to destroy it, to capture a regiment, a detachment, or a company entire than to destroy it."[1]

What does this paragraph say to a system administrator or security officer seeking insight to defend her systems?

Outline for the Day

1. Public-Key Cryptography
   a. Basic idea: 2 keys, one private, one public
   b. Cryptosystem must satisfy:
      i. given public key, CI to get private key;
      ii. cipher withstands chosen plaintext attack;
      iii. encryption, decryption computationally feasible [note: commutativity ***not*** required]
   c. Benefits: can give confidentiality or authentication or both
2. RSA
   a. Provides both authenticity and confidentiality
   b. Go through algorithm:
      Idea: $C = M^e \bmod n$, $M = C^d \bmod n$, with $ed \bmod \phi(n) = 1$.
      Proof: $M^{\phi(n)} \bmod n = 1$ [by Fermat's theorem as generalized by Euler]; follows immediately from $ed \bmod \phi(n) = 1$.
      Public key is (e, n); private key is d. Choose $n = pq$; then $\phi(n) = (p-1)(q-1)$.
   c. Example:
      $p = 5$, $q = 7$; $n = 35$, $\phi(n) = (5-1)(7-1) = 24$. Pick $e = 11$. Then $ed \bmod \phi(n) = 1$, so choose $d = 11$. To encipher 2, $C = M^e \bmod n = 2^{11} \bmod 35 = 2048 \bmod 35 = 18$, and $M = C^d \bmod n = 18^{11} \bmod 35 = 2$.
   d. Example: $p = 53$, $q = 61$, $n = 3233$, $\phi(n) = (53-1)(61-1) = 3120$. Take $e = 71$; then $d = 791$. Encipher M = RENAISSANCE: A = 00, B = 01, …, Z = 25, blank = 26. Then:
      M = RE NA IS SA NC Eblank = 1704 1300 0818 1800 1302 0426
      $C = (1704)^{71} \bmod 3233 = 3106$; etc. = 3106 0100 0931 2691 1984 2927
3. Cryptographic Checksums
   a. Function $y = h(x)$: easy to compute y given x; computationally infeasible to compute x given y
   b. Variant: given x and y, computationally infeasible to find a second x' such that $y = h(x')$.
   c. Keyed vs. keyless

1. Sun Tzu, *The Art of War*, James Clavell, *ed*., Dell Publishing, New York, NY ©1983, p. 15